BlackBoxLab1

nmap -T4 -p- -A 172.16.64.0/24 130

```
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-11 17:41 EDT
Nmap scan report for 172.16.64.101
Host is up (0.044s latency).
Not shown: 65531 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 7f:b7:1c:3d:55:b3:9d:98:58:11:17:ef:cc:af:27:67 (RSA)
|   256 5f:b9:93:e2:ec:eb:f7:08:e4:bb:82:d0:df:b9:b1:56 (ECDSA)
|_  256 db:1f:11:ad:59:c1:3f:0c:49:3d:b0:66:10:fa:57:21 (ED25519)
8080/tcp  open  http    Apache Tomcat/Coyote JSP engine 1.1
| http-methods:
|_  Potentially risky methods: PUT DELETE
|_http-server-header: Apache-Coyote/1.1
|_http-title: Apache2 Ubuntu Default Page: It works
9080/tcp  open  http    Apache Tomcat/Coyote JSP engine 1.1
| http-methods:
|_  Potentially risky methods: PUT DELETE
|_http-server-header: Apache-Coyote/1.1
|_http-title: Apache2 Ubuntu Default Page: It works
59919/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
MAC Address: 00:50:56:A2:AF:8F (VMware)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/-
submit/ ).



Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT      ADDRESS
1   44.27 ms 172.16.64.101

Nmap scan report for 172.16.64.140
Host is up (0.032s latency).
Not shown: 65534 closed ports
PORT   STATE SERVICE VERSION
```

80/tcp open http   Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: 404 HTML Template by Colorlib
MAC Address: 00:50:56:A2:59:6D (VMware)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/-submit/).

Network Distance: 1 hop

TRACEROUTE
HOP RTT   ADDRESS
1   32.34 ms 172.16.64.140

Nmap scan report for 172.16.64.182
Host is up (0.033s latency).
Not shown: 65534 closed ports
PORT   STATE SERVICE VERSION
22/tcp open ssh   OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
| 2048 7f:b7:1c:3d:55:b3:9d:98:58:11:17:ef:cc:af:27:67 (RSA)
| 256 5f:b9:93:e2:ec:eb:f7:08:e4:bb:82:d0:df:b9:b1:56 (ECDSA)
|_ 256 db:1f:11:ad:59:c1:3f:0c:49:3d:b0:66:10:fa:57:21 (ED25519)
MAC Address: 00:50:56:A2:91:6A (VMware)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/-submit/).

Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT   ADDRESS
1   33.20 ms 172.16.64.182

Nmap scan report for 172.16.64.199
Host is up (0.031s latency).
Not shown: 65522 closed ports
PORT   STATE SERVICE   VERSION
135/tcp   open msrpc   Microsoft Windows RPC
139/tcp   open netbios-ssn   Microsoft Windows netbios-ssn
445/tcp   open microsoft-ds?
1433/tcp open ms-sql-s   Microsoft SQL Server 2014 12.00.2000.00; RTM
| ms-sql-ntlm-info:

| Target_Name: WIN10
| NetBIOS_Domain_Name: WIN10
| NetBIOS_Computer_Name: WIN10
| DNS_Domain_Name: WIN10
| DNS_Computer_Name: WIN10
|_ Product_Version: 10.0.10586
| ssl-cert: Subject: commonName=SSL_Self_Signed_Fallback
| Not valid before: 2021-06-11T17:16:00
|_Not valid after: 2051-06-11T17:16:00
|_ssl-date: 2021-06-11T21:46:46+00:00; +1s from scanner time.
7680/tcp open pando-pub?
49664/tcp open msrpc   Microsoft Windows RPC
49665/tcp open msrpc   Microsoft Windows RPC
49666/tcp open msrpc   Microsoft Windows RPC
49667/tcp open msrpc   Microsoft Windows RPC
49668/tcp open msrpc   Microsoft Windows RPC
49669/tcp open msrpc   Microsoft Windows RPC
49670/tcp open msrpc   Microsoft Windows RPC
49943/tcp open ms-sql-s   Microsoft SQL Server 2014 12.00.2000
| ms-sql-ntlm-info:
| Target_Name: WIN10
| NetBIOS_Domain_Name: WIN10
| NetBIOS_Computer_Name: WIN10
| DNS_Domain_Name: WIN10
| DNS_Computer_Name: WIN10
|_ Product_Version: 10.0.10586
| ssl-cert: Subject: commonName=SSL_Self_Signed_Fallback
| Not valid before: 2021-06-11T17:16:00
|_Not valid after: 2051-06-11T17:16:00
|_ssl-date: 2021-06-11T21:46:46+00:00; +2s from scanner time.
MAC Address: 00:50:56:A2:BE:5F (VMware)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/-submit/).

Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: 1s, deviation: 0s, median: 1s
| ms-sql-info:
| 172.16.64.199:1433:
| Version:
| name: Microsoft SQL Server 2014 RTM
| number: 12.00.2000.00

```
|       Product: Microsoft SQL Server 2014
|       Service pack level: RTM
|       Post-SP patches applied: false
|_    TCP port: 1433
|_nbstat: NetBIOS name: WIN10, NetBIOS user: <unknown>, NetBIOS MAC: 00:50:56:a2:be:-
5f (VMware)
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2021-06-11T21:46:42
|_  start_date: 2021-06-11T17:15:57

TRACEROUTE
HOP RTT      ADDRESS
1   31.17 ms 172.16.64.199

Nmap scan report for 172.16.64.10
Host is up (0.000025s latency).
All 65535 scanned ports on 172.16.64.10 are closed
Too many fingerprints match this host to give specific OS details
Network Distance: 0 hops

Post-scan script results:
| ssh-hostkey: Possible duplicate hosts
| Key 2048 7f:b7:1c:3d:55:b3:9d:98:58:11:17:ef:cc:af:27:67 (RSA) used by:
|   172.16.64.101
|   172.16.64.182
| Key 256 db:1f:11:ad:59:c1:3f:0c:49:3d:b0:66:10:fa:57:21 (ED25519) used by:
|   172.16.64.101
|   172.16.64.182
| Key 256 5f:b9:93:e2:ec:eb:f7:08:e4:bb:82:d0:df:b9:b1:56 (ECDSA) used by:
|   172.16.64.101
|_  172.16.64.182
```